

National Cyber Alert System

Cyber Security Bulletin SB09-215

[Archive](#)

Vulnerability Summary for the Week of July 27, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- catalyst_3750g cisco -- cisco_1500_wireless_lan_controller cisco -- cisco_2000_wireless_lan_controller cisco -- cisco_2100_wireless_lan_controller cisco -- cisco_4100_wireless_lan_controller cisco -- cisco_4200_wireless_lan_controller cisco -- cisco_4400_wireless_lan_controller	The administrative web interface on the Cisco Wireless LAN Controller (WLC) platform 4.2 before 4.2.205.0 and 5.x before 5.2.178.0, as used in Cisco 1500 Series, 2000 Series, 2100 Series, 4100 Series, 4200 Series, and 4400 Series Wireless Services Modules (WiSM), WLC Modules for Integrated Services Routers, and Catalyst 3750G Integrated Wireless LAN Controllers, allows remote attackers to cause a denial of service (device reload) via a malformed response to a (1) HTTP or (2) HTTPS authentication request, aka Bug ID CSCsx03715.	2009-07-29	7.8	CVE-2009-1164 CISCO
cisco -- catalyst_3750g cisco -- cisco_1500_wireless_lan_controller cisco -- cisco_2000_wireless_lan_controller cisco -- cisco_2100_wireless_lan_controller cisco -- cisco_4100_wireless_lan_controller cisco --	Memory leak on the Cisco Wireless LAN Controller (WLC) platform 4.x before 4.2.205.0, 5.1 before 5.1.163.0, and 5.0 and 5.2 before 5.2.178.0, as used in Cisco 1500 Series, 2000 Series, 2100 Series, 4100 Series, 4200 Series, and 4400 Series Wireless Services Modules (WiSM), WLC Modules for Integrated Services Routers, and Catalyst 3750G Integrated Wireless LAN Controllers, allows remote attackers to cause a denial of service (memory	2009-07-29	7.8	CVE-2009-1165 CISCO

cisco_4200_wireless_lan_controller cisco -- cisco_4400_wireless_lan_controller	consumption and device reload) via SSH management connections, aka Bug ID CSCsw40789.			
cisco -- catalyst	The administrative web interface on the Cisco Wireless LAN Controller (WLC) platform 4.x before 4.2.205.0 and 5.x before 5.2.191.0, as used in Cisco 1500 Series, 2000 Series, 2100 Series, 4100 Series, 4200 Series, and 4400 Series Wireless Services Modules (WiSM), WLC Modules for Integrated Services Routers, and Catalyst 3750G Integrated Wireless LAN Controllers, allows remote attackers to cause a denial of service (device reload) via a crafted (1) HTTP or (2) HTTPS request, aka Bug ID CSCsy27708.	2009-07-29	7.8	CVE-2009-1166 CISCO
cisco -- catalyst_3750g cisco -- cisco_1500_wireless_lan_controller cisco -- cisco_2000_wireless_lan_controller cisco -- cisco_2100_wireless_lan_controller cisco -- cisco_4100_wireless_lan_controller cisco -- cisco_4200_wireless_lan_controller cisco -- cisco_4400_wireless_lan_controller	Unspecified vulnerability on the Cisco Wireless LAN Controller (WLC) platform 4.x before 4.2.205.0 and 5.x before 5.2.191.0, as used in Cisco 1500 Series, 2000 Series, 2100 Series, 4100 Series, 4200 Series, and 4400 Series Wireless Services Modules (WiSM), WLC Modules for Integrated Services Routers, and Catalyst 3750G Integrated Wireless LAN Controllers, allows remote attackers to modify the configuration via a crafted (1) HTTP or (2) HTTPS request, aka Bug ID CSCsy44672.	2009-07-29	10.0	CVE-2009-1167 CISCO
cisco -- ios cisco -- ios_xe	Cisco IOS 12.0(32)S12 through 12.0(32)S13 and 12.0(33)S3 through 12.0(33)S4, 12.0(32)SY8 through 12.0(32)SY9, 12.2(33)SXI1, 12.2XNC before 12.2(33)XNC2, 12.2XND before 12.2(33)XND1, and 12.4(24)T1; and IOS XE 2.3 through 2.3.1t and 2.4 through 2.4.0; when RFC4893 BGP routing is enabled, allows remote attackers to cause a denial of service (memory corruption and device reload) by using an RFC4271 peer to send an update with a long series of AS numbers, aka Bug ID CSCsy86021.	2009-07-30	7.1	CVE-2009-1168 CISCO
desiscripts -- desi_short_url_script	index.php in Desi Short URL Script 1.0 allows remote attackers to bypass authentication by setting the logged cookie to 1 and the uid cookie to an integer value, as demonstrated by a value of 13.	2009-07-28	7.5	CVE-2009-2642 MILWORM
easysitenetwork -- jokes_complete_website	SQL injection vulnerability in joke.php in EasySiteNetwork Free Jokes Website allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-07-30	7.5	CVE-2008-6880 XF BID BUGTRAQ OSVDB
fedorahosted -- sssd	The local_handler_callback function in server/responder/pam/pam_LOCAL_domain.c in sssd 0.4.1 does not properly handle blank-password accounts in the SSSD BE database, which allows context-dependent attackers to obtain access by sending the account's username, in conjunction with an arbitrary password, over an ssh connection.	2009-07-30	7.5	CVE-2009-2410 FEDORA CONFIRM CONFIRM BID SECUNIA
hp -- proliant_dl120 hp -- proliant_dl160 hp -- proliant_dl165	Unspecified vulnerability on HP ProLiant DL and ML			

hp -- proliant_dl180 hp -- proliant_dl185 hp -- proliant_ml110 hp -- proliant_ml115 hp -- proliant_ml150 hp -- proliant_onboard_administrator	100 Series G5, G5p, and G6 servers with ProLiant Onboard Administrator Powered by LO100i (formerly Lights Out 100) 3.07 and earlier allows remote attackers to cause a denial of service via unknown vectors.	2009-07-29	7.8	CVE-2009-1426 HP HP
interlogy -- profile_manager	Multiple SQL injection vulnerabilities in cgi/admin.cgi in Interlogy Profile Manager Basic allow remote attackers to execute arbitrary SQL commands via a pmadm cookie in (1) an edittemp action or (2) a users action.	2009-07-28	7.5	CVE-2009-2640 XF VUPEN MILWoRM
joompolitan -- com_livechat	Multiple SQL injection vulnerabilities in the Live Chat (com_livechat) component 1.0 for Joomla! allow remote attackers to execute arbitrary SQL commands via the last parameter to (1) getChat.php, (2) getChatRoom.php, and (3) getSavedChatRooms.php.	2009-07-30	7.5	CVE-2008-6881 BID
joompolitan -- com_livechat	Live Chat (com_livechat) component 1.0 for Joomla! allows remote attackers to use the xmlhttp.php script as an open HTTP proxy to hide network scanning activities or scan internal networks via a GET request with a full URL in the query string.	2009-07-30	7.5	CVE-2008-6882 XF BID MILWoRM
joompolitan -- com_livechat	SQL injection vulnerability in the Live Chat (com_livechat) component 1.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the last parameter to getChatRoom.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-07-30	7.5	CVE-2008-6883 XF BID MILWoRM SECUNIA
konze -- com_akobook	SQL injection vulnerability in the AkoBook (com_akobook) component 2.3 for Joomla! allows remote attackers to execute arbitrary SQL commands via the gbid parameter in a reply action to index.php.	2009-07-28	7.5	CVE-2009-2638 BID MILWoRM
microsoft -- visual_c++ microsoft -- visual_studio microsoft -- visual_studio_.net	The Active Template Library (ATL) in Microsoft Visual Studio .NET 2003 SP1, Visual Studio 2005 SP1 and 2008 Gold, and Visual C++ 2005 SP1 and 2008 Gold and SP1 does not prevent VariantClear calls on an uninitialized VARIANT, which allows remote attackers to execute arbitrary code via a malformed stream to an ATL (1) component or (2) control, related to ATL headers and error handling, aka "ATL Uninitialized Object Vulnerability."	2009-07-29	9.3	CVE-2009-0901 BID CONFIRM CONFIRM
microsoft -- ie microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft Internet Explorer 6 SP1; Internet Explorer 6 for Windows XP SP2 and SP3 and Server 2003 SP2; and Internet Explorer 7 and 8 for Windows XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 do not properly handle attempts to access deleted objects in memory, which allows remote attackers to execute arbitrary code via a crafted HTML document that triggers memory corruption, aka "Memory Corruption Vulnerability."	2009-07-29	9.3	CVE-2009-1917 MS
microsoft -- ie microsoft -- windows_2000 microsoft -- windows_server_2003	Microsoft Internet Explorer 5.01 SP4 and 6 SP1; Internet Explorer 6 for Windows XP SP2 and SP3 and Server 2003 SP2; and Internet Explorer 7 and 8 for Windows XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and	2009-07-29	10.0	CVE-2009-1919

microsoft -- windows_server_2003 microsoft -- windows_vista microsoft -- windows_xp	SP2 do not properly handle table operations, which allows remote attackers to execute arbitrary code via a crafted HTML document that triggers memory corruption, aka "HTML Objects Memory Corruption Vulnerability."	29	10.0	2009-1910 MS
microsoft -- ie microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft Internet Explorer 5.01 SP4 and 6 SP1; Internet Explorer 6 for Windows XP SP2 and SP3 and Server 2003 SP2; and Internet Explorer 7 and 8 for Windows XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 do not properly handle attempts to access deleted objects in memory, which allows remote attackers to execute arbitrary code via a crafted HTML document that triggers memory corruption, aka "Uninitialized Memory Corruption Vulnerability."	2009-07-29	9.3	CVE-2009-1919 MS
microsoft -- visual_c++ microsoft -- visual_studio microsoft -- visual_studio_.net	The Active Template Library (ATL) in Microsoft Visual Studio .NET 2003 SP1, Visual Studio 2005 SP1 and 2008 Gold and SP1, and Visual C++ 2005 SP1 and 2008 Gold and SP1 does not properly restrict use of OleLoadFromStream in instantiating objects from data streams, which allows remote attackers to execute arbitrary code via a crafted HTML document with an ATL (1) component or (2) control, related to ATL headers and bypassing security policies, aka "ATL COM Initialization Vulnerability."	2009-07-29	9.3	CVE-2009-2493 MS CONFIRM CONFIRM
microsoft -- visual_c++ microsoft -- visual_studio microsoft -- visual_studio_.net	The Active Template Library (ATL) in Microsoft Visual Studio .NET 2003 SP1, Visual Studio 2005 SP1 and 2008 Gold and SP1, and Visual C++ 2005 SP1 and 2008 Gold and SP1 does not properly enforce string termination, which allows remote attackers to obtain sensitive information via a crafted HTML document with an ATL (1) component or (2) control that triggers a buffer over-read, related to ATL headers and buffer allocation, aka "ATL Null String Vulnerability."	2009-07-29	7.8	CVE-2009-2495 MS
mozilla -- firefox mozilla -- nss	Mozilla Firefox before 3.5 and NSS before 3.12.3 do not properly handle a '\o' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.	2009-07-30	7.5	CVE-2009-2408 CONFIRM MISC
mrcgiguy -- the_ticket_system	SQL injection vulnerability in admin.php in MRCGIGUY The Ticket System 2.0 allows remote attackers to execute arbitrary SQL commands via the id parameter in a viewticket action.	2009-07-28	7.5	CVE-2009-2639 MILWORM
ordasoft -- com_vehiclemanager	PHP remote file inclusion vulnerability in toolbar_ext.php in the VehicleManager (com_vehiclemanager) component 1.0 Basic for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter.	2009-07-28	7.5	CVE-2009-2633 MILWORM
ordasoft -- com_medialibrary	PHP remote file inclusion vulnerability in toolbar_ext.php in the MediaLibrary (com_media_library) component 1.5.3 Basic for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path	2009-07-28	7.5	CVE-2009-2634 MILWORM

	parameter.			
ordasoft -- com_realestatemanager	PHP remote file inclusion vulnerability in toolbar_ext.php in the RealEstateManager (com_realestatemanager) component 1.0 Basic for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter.	2009-07-28	7.5	CVE-2009-2635 MILWORM
ordasoft -- com_booklibrary	PHP remote file inclusion vulnerability in toolbar_ext.php in the BookLibrary (com_booklibrary) component 1.5.2.4 Basic for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter.	2009-07-28	7.5	CVE-2009-2637 MILWORM
rim -- blackberry_enterprise_server rim -- blackberry_professional_software	Multiple unspecified vulnerabilities in the PDF distiller in the Attachment Service component in Research In Motion (RIM) BlackBerry Enterprise Server (BES) software 4.1.3 through 5.0 and BlackBerry Professional Software 4.1.4 allow user-assisted remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted .pdf file attachment, a different vulnerability than CVE-2008-3246 and CVE-2009-0219.	2009-07-28	9.3	CVE-2009-2643 VUPEN CONFIRM
rim -- blackberry_enterprise_server rim -- blackberry_professional_software	Multiple unspecified vulnerabilities in the PDF distiller in the Attachment Service component in Research In Motion (RIM) BlackBerry Enterprise Server (BES) software 4.1.3 through 4.1.6 and BlackBerry Professional Software 4.1.4 allow user-assisted remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted .pdf file attachment, a different vulnerability than CVE-2008-3246 and CVE-2009-0219.	2009-07-30	9.3	CVE-2009-2646 CONFIRM
sorcerersoftware -- multimedia_jukebox	Heap-based buffer overflow in Sorcerer Software MultiMedia Jukebox 4.0 Build 020124 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted (1) .m3u or possibly (2) .pst file.	2009-07-30	7.5	CVE-2009-2650 MILWORM SECUNIA

[Back to top](#)

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- roller	Cross-site scripting (XSS) vulnerability in Apache Roller 2.3, 3.0, 3.1, and 4.0 allows remote attackers to inject arbitrary web script or HTML via the q parameter in a search action.	2009-07-30	4.3	CVE-2008-6879 BID CONFIRM CONFIRM
asterisk -- open_source	main/rtp.c in Asterisk Open Source 1.6.1 before 1.6.1.2 allows remote attackers to cause a denial of service (crash) via an RTP text frame without a certain delimiter, which triggers a NULL pointer dereference and the subsequent calculation of an invalid pointer.	2009-07-30	5.0	CVE-2009-2651 XF VUPEN SECTRACK BID SECUNIA OSVDB MISC

				CONFIRM
chatelao -- php_address_book	Multiple SQL injection vulnerabilities in PHP Address Book 4.0.x allow remote attackers to execute arbitrary SQL commands via the (1) id parameter to delete.php and (2) alphabet parameter to index.php. NOTE: the edit.php and view.php vectors are already covered by CVE-2008-2565.	2009-07-27	6.8	CVE-2009-2608 BID MILWoRM SECUNIA
cisco -- ios cisco -- ios_xe	Cisco IOS 12.0(32)S12 through 12.0(32)S13 and 12.0(33)S3 through 12.0(33)S4, 12.0(32)SY8 through 12.0(32)SY9, 12.2(33)SXI1 through 12.2(33)SXI2, 12.2XNC before 12.2(33)XNC2, 12.2XND before 12.2(33)XND1, and 12.4(24)T1; and IOS XE 2.3 through 2.3.1t and 2.4 through 2.4.0; when RFC4893 BGP routing is enabled, allows remote attackers to cause a denial of service (device reload) by using an RFC4271 peer to send a malformed update, aka Bug ID CSCta33973.	2009-07-30	4.0	CVE-2009-2049 CISCO
firebirdsql -- firebird	src/remote/server.cpp in fbserver.exe in Firebird SQL 1.5 before 1.5.6, 2.0 before 2.0.6, 2.1 before 2.1.3, and 2.5 before 2.5 Beta 2 allows remote attackers to cause a denial of service (daemon crash) via a malformed op_connect_request message that triggers an infinite loop or NULL pointer dereference.	2009-07-29	5.0	CVE-2009-2620 BID
flashden -- guestbook	FlashDen Guestbook allows remote attackers to obtain configuration information via a direct request to amfphp/phpinfo.php, which calls the phpinfo function.	2009-07-30	5.0	CVE-2009-2648 XF SECUNIA MISC OSVDB
freebsd -- freebsd	The IATA (ata) driver in FreeBSD 6.0 and 8.0, when read access to /dev is available, allows local users to cause a denial of service (kernel panic) via a certain IOCTL request with a large count, which triggers a malloc call with a large value.	2009-07-30	4.7	CVE-2009-2649 SECTRACK MILWORM
isc -- bind	The dns_db_findrdataset function in db.c in named in ISC BIND 9.4 before 9.4.3-P3, 9.5 before 9.5.1-P3, and 9.6 before 9.6.1-P1, when configured as a master server, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via an ANY record in the prerequisite section of a crafted dynamic update message, as exploited in the wild in July 2009.	2009-07-29	4.3	CVE-2009-0696 CERT-VN
kaspersky -- kaspersky_antivirus kaspersky -- kaspersky_internet_security	Unspecified vulnerability in Kaspersky Anti-Virus 2010 and Kaspersky Internet Security 2010 before Critical Fix 9.0.0.463 allows remote attackers to disable the Kaspersky application via unknown attack vectors unrelated to "an external script."	2009-07-30	5.0	CVE-2009-2647 XF VUPEN BID CONFIRM SECUNIA OSVDB
kerio -- kerio_mailserver	Cross-site scripting (XSS) vulnerability in the Integration page in the WebMail component in Kerio MailServer 6.6.0, 6.6.1, 6.6.2, and 6.7.0 allows remote attackers to inject arbitrary web script or HTML via an e-mail message.	2009-07-28	4.3	CVE-2009-2636 SECTRACK BID
mozilla -- nss	The NSS library before 3.12.3, as used in Firefox; GnuTLS before 2.6.4 and 2.7.4; OpenSSL 0.9.8 through 0.9.8k; and other products support MD2 with X.509 certificates, which might allow remote attackers to spoof certificates	2009-07-28	5.0	CVE-2009-2620 BID

openssl -- openssl	by using MD2 design flaws to generate a hash collision in less than brute-force time. NOTE: the scope of this issue is currently limited because the amount of computation required is still large.	30	5.0	2409 CONFIRM
rich_white -- school_data_nav	PHP remote file inclusion vulnerability in app_and_readme/navigator/index.php in School Data Navigator allows remote attackers to execute arbitrary PHP code via a URL in the page parameter. NOTE: this can also be leveraged to include and execute arbitrary local files via .. (dot dot) sequences.	2009-07-28	6.8	CVE-2009-2641 MILWoRM
squid-cache -- squid	Squid 3.0 through 3.0.STABLE16 and 3.1 through 3.1.0.11 does not properly enforce "buffer limits and related bound checks," which allows remote attackers to cause a denial of service via (1) an incomplete request or (2) a request with a large header size, related to (a) HttpMsg.cc and (b) client_side.cc.	2009-07-28	5.0	CVE-2009-2621 CONFIRM
squid-cache -- squid	Squid 3.0 through 3.0.STABLE16 and 3.1 through 3.1.0.11 allows remote attackers to cause a denial of service via malformed requests including (1) "missing or mismatched protocol identifier," (2) missing or negative status value," (3) "missing version," or (4) "missing or invalid status number," related to (a) HttpMsg.cc and (b) HttpReply.cc.	2009-07-28	5.0	CVE-2009-2622 CONFIRM
sun -- opensolaris sun -- solaris	Race condition in the Solaris Auditing subsystem in Sun Solaris 9 and 10 and OpenSolaris before snv_121, when extended file attributes are used, allows local users to cause a denial of service (panic) via vectors related to "pathnames for invalid fds."	2009-07-29	4.9	CVE-2009-2644 SUNALERT CONFIRM
zen_cart -- zen_cart	** DISPUTED ** Directory traversal vulnerability in admin/includes/initSystem.php in Zen Cart 1.3.8 and 1.3.8a, when .htaccess is not supported, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the loader_file parameter. NOTE: the vendor disputes this issue, stating "at worst, the use of this vulnerability will reveal some local file paths."	2009-07-27	6.8	CVE-2008-6877 MISC BID MILWoRM VIM SECUNIA OSVDB
zen_cart -- zen_cart	** DISPUTED ** Directory traversal vulnerability in admin/includes/languages/english.php in Zen Cart 1.3.8a, 1.3.8, and earlier, when .htaccess is not supported, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the _SESSION[language] parameter. NOTE: the vendor disputes this issue, stating "at worst, the use of this vulnerability will reveal some local file paths."	2009-07-27	6.8	CVE-2008-6878 MISC BID MILWoRM VIM SECUNIA OSVDB

[Back to top](#)

There were no low vulnerabilities recorded this week.

Last updated August 03, 2009

 Print This Document